誤り訂正符号の復号における確率伝搬アルゴリズム : 理論的特性限界へのアプローチ(多体問題としての情報処理-統計力学と情報科学の接点-,研究会報告)

AUTHOR(S):

井坂, 元彦; 今井, 秀樹

CITATION:

井坂, 元彦 ...[et al]. 誤り訂正符号の復号における確率伝搬アルゴリズム : 理論的特性限界へのアプローチ(多体問題としての情報処理-統計力学と情報科学の接点-,研究会報告). 物性研究 2000, 73(5): 828-833

ISSUE DATE:

2000-02-20

URL:

http://hdl.handle.net/2433/96786

誤り訂正符号の復号における確率伝搬アルゴリズム

— 理論的特性限界へのアプローチ —

東京大学 生産技術研究所　井坂 元彦[1]，今井 秀樹[2]

1 まえがき

符号理論研究は，1948 年の Shannon による情報理論の創設 [1] を起源とし，その産物は通信の信頼性向上に不可欠の技術として既に多くの局面で実用化されている．Shannon の通信路符号化定理によれば，与えられた伝送路に対して通信路容量が定義され，伝送速度がこれを超えない限りは，適当な符号化により任意に誤り数を小さくできる．その証明過程から知られる通り，長い符号長を有し，かつランダム的な構成の符号の大部分が優れた特性を示すことは情報理論の根源的概念となってきた．しかし，この種の符号は，最適な復号に要する計算量及び記憶素子が符号長に対して指数的に増大するため，高度に構造を有する代数的符号の構成が長年の符号理論の中心課題となっていた．その結果，実用的とされていた符号は理論特性限界には遠く及ばず，この意味において，工学的に“よい”符号は構成不可能との認識が浸透していたのである．

これに対し，1993 年に提案された Turbo 符号は，従来見逃されていた符号の重要な設計規範を突いて，過去に例を見ない優れたビット誤り率 (BER) を示す長くランダム的な符号の構成法を提示した．さらに，複数の復号器を用いた反復的かつ確率的手法により符号長に比例する複雑度にて復号することに成功したのである．その後，反復復号手法は人工知能分野における確率伝搬アルゴリズムに帰着されることが指摘され，さらに約 35 年前に提案されていた低密度パリティ検査符号 [3] の再発見と併せて，グラフ上で定義される符号及び復号に興味が高まりつつある．

本稿では，Turbo 符号を中心とした確率的な復号アルゴリズムに関する話題を概説する．

2 Turbo 符号，反復復号法

$GF(2)$ 上の長さ N のメッセージ系列 $\boldsymbol{u} = (u_1, u_2, \cdot\cdot, u_k, \cdot\cdot, u_N)$: $u_k \in \{\pm 1\}$ [3] を符号化の後，伝達を試みるとする．レート N/N' $(N < N')$ の符号化を仮定すると，$\boldsymbol{u}$ に応じて $\boldsymbol{x}_j$ $(1 \leq j \leq 2^N)$ が N' 次元空間中の 2^N の符号語の中から選択されて，通信路に伝送される．$\boldsymbol{x}_j = (x_1, x_2, \cdot\cdot, x_k, \cdot\cdot, x_{N'})$ $x_k \in \{\pm 1\}$ に対応する雑音が加えられた受信系列を $\boldsymbol{y} = (y_1, y_2, \cdots, y_{N'})$ と書くと，この符号に対する復号は必然的に $\boldsymbol{y}$ に基づいて $\boldsymbol{u}$ を効率的に推定する問題に帰着される．以下 $\hat{\boldsymbol{u}} = (\hat{u}_1, \hat{u}_2, \cdot\cdot, \hat{u}_N)$ を復号による推定情報系列とする．

[1]研究機関研究員, isaka@imailab.iis.u-tokyo.ac.jp
[2]教授. imai@iis.u-tokyo.ac.jp
[3]$0 \rightarrow +1$, $1 \rightarrow -1$ とする

従来，最も重視されてきた符号設計規範は，符号長 N 及びレート N/N' が与えられた際の，異なる符号語間の最小 Hamming 距離 d_{min} の最大化であった[4]．この設計規範は，高 SNR（信号対雑音電力比）において最適な指針を与える一方で，雑音の厳しい環境で良好な特性を得るには d_{min} が小さい範囲の誤り事象数を低減させることが必要となるが，Turbo 符号の特性の鍵は長年見逃されていたこの事実を突いたことにある．

Turbo 符号化器の構造は図 1(a) に示すように，複数（図中では 2 個）の符号化器を並列連接 (parallel concatenation) したものである．N ビットの情報系列 $\boldsymbol{i} = (i_1, i_2, \cdots, i_N)$ と（ランダム）インタリーバを通過した置換系列 $\boldsymbol{i}' = (i'_1, i'_2, \cdots, i'_N)$ はともに図 1(b) のレート 1/2 の再帰的組織畳み込み（以下，RSC: Recursive Systematic Convolutional）符号化器 *encoder1*,*encoder2* によってそれぞれ符号化される．

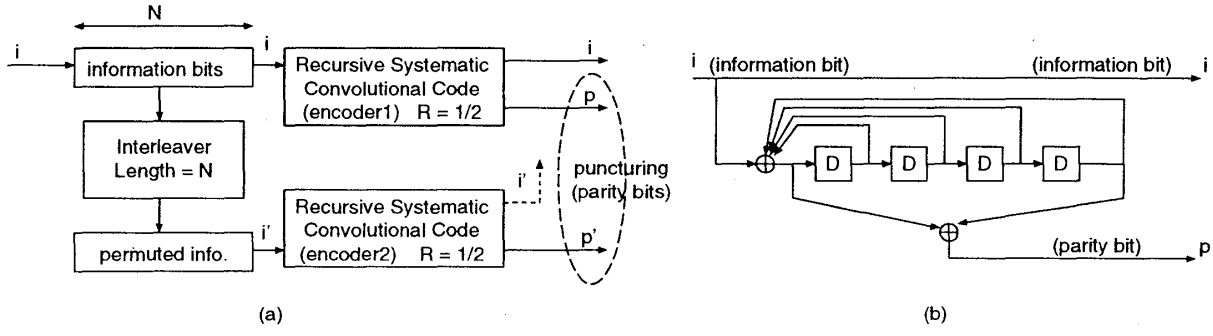

図 1: (a) Turbo 符号の符号化器, (b) 再帰的組織畳み込み符号化器 (Recursive Systematic Convolutional Code): レート 1/2, (a) $d_0(D) = 1 + D + D^2 + D^3 + D^4$, $d_1(D) = 1 + D^4$

直感的には，単一のメッセージ系列に対してインタリーバによる置換系列を生成し，それぞれに振る舞いの異なるパリティ系列を付与することで，総体としての符号をランダム化を図っていると解釈できる．ここで，Turbo 符号では RSC 符号 (IIR 型) が用いられている[5]のは，符号化器内に帰還タップが存在するために，成分符号化器へのメッセージ系列 $\boldsymbol{i}$ と置換された $\boldsymbol{i}'$ に対して，両符号化器から生成されるパリティ系列 $\boldsymbol{p}$ と $\boldsymbol{p}'$ の Hamming 重みがともに小さくなることが確率的に小さいためである[6]．このため，両符号化器出力のパリティ系列を並列的に組み合わせることで符号の Hamming 重みの分布が 2 項分布に近いものとなり，ランダム的な符号が構成される．なお上で述べたように発生確率は大きくはないが，Turbo 符号の d_{min} は相対的に小さく，従来の符号設計規範と大きく食い違うことが理解される．複数の符号を組み合わせにより強力な符号を構成する手法は，以前から符号理論の基本的手法ではあったものの，その代表例である 2 元符号と拡大体上の符号の縦列連接符号化では基本的に d_{min} を最適化しており，かつ反復復号的な概念も想起しにくいといった事情から，Turbo 符号復号のような考え方に結び付かなかった．

[4]Hamming 距離は符号語同士で異なるビット位置の総数，Hamming 重みは全零符号語との Hamming 距離と定義する

[5]従来，符号理論で用いられてきた畳込み符号は大部分が帰還のない FIR 型の符号化器であった

[6]例えば，単一誤りに対して，パリティ出力は無限の応答を示す

ランダム化の結果として，図2[7]に示される通り低SNRでのBER特性は大幅に改善される．但し，雑音電力が一定値以上であると，次章で述べる反復復号が機能せず，アルゴリズムの収束に関するある臨界点を越えた時点でBER特性が急速に下落する減少が見られる（ウォーターフォール領域）．一方で，Turbo符号自体の性能限界に至ると，BERは緩やかな減少傾向を示し，BERの急落減少と対比的にエラーフロア領域と呼ばれる．すなわちエラーフロア領域では，反復復号によってほぼ最適な復号が実現されていると解釈できるのである．なお，エラーフロア領域におけるBER値はNに反比例することが知られている．

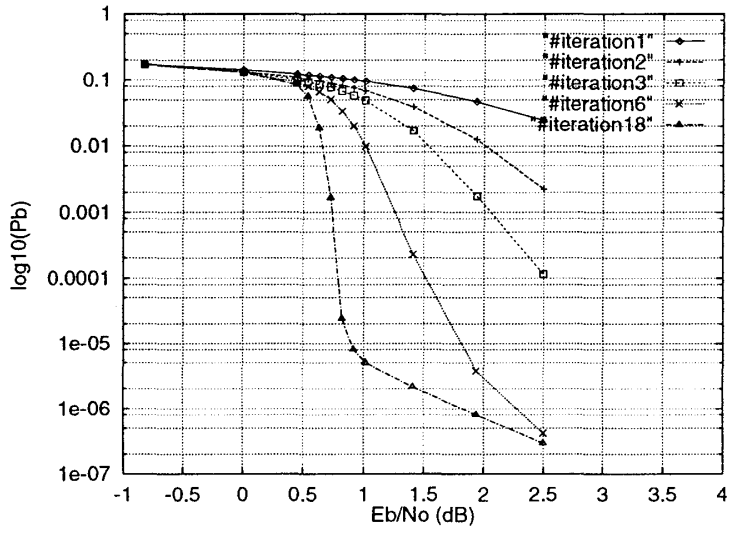

図 2: 各反復回数における Turbo 符号の BER 特性 (E_b/N_0: ビット単位の信号対雑音電力比, Pb: ビット誤り率)

3 反復復号法

$P(\boldsymbol{y}|\boldsymbol{x}_j)$ $1 \leq j \leq 2^N$の最大値を与える$\boldsymbol{u}$を情報系列として推定する復号規範は最尤 (ML: Maximum Likelihood) 復号と呼ばれる．これはブロック誤り確率を最小化するという意味で最適な復号法であり，Viterbiアルゴリズムによって効率的に実現されるため，復号に留まらず，伝送システムにおけるあらゆる信号検出問題がML復号規範により扱われてきた．

しかし，ビット（シンボル）誤り率の最小化という観点からは最尤復号は最適ではなく，最大事後確率 (MAP: Maximum *a posteriori* Probability) 復号の導入が必要となる．MAP復号は受信信号系列$\boldsymbol{y}$が与えられた条件下で，各情報シンボルu_k $(1 \leq k \leq N)$に関して対数尤度比 (LLR: Log-Likelihood Ratio) $L(\hat{u}_k)$

$$L(\hat{u}_k) = L(u_k|\boldsymbol{y}) = \ln \frac{P(u_k = +1|\boldsymbol{y})}{P(u_k = -1|\boldsymbol{y})}, \tag{1}$$

[7] N=16384，パリティ系列のパンクチャによるレート 1/2 の Turbo 符号のガウス性通信路における特性．2元の伝送を行なった場合，Shannon限界は$0.2dB$であるため，ビット誤り率10^{-5}を理論限界から$0.5-0.6dB$で達成している．#iteration$\star$は$\star$回目の反復時における BER 特性を示す．

を評価する．MAP復号はViterbiアルゴリズムに比して計算コストが大きいが，単一の符号に適用された際，BER特性の改善度合が限られてるため殆ど用いられてこなかった．

一定長以上のTurbo符号に対する最尤復号は，必要とされる計算量や記憶素子の面からほぼ不可能であるが，この意味において復号複雑度が高く長い符号を，複雑度の小さい複数の要素に分解し，各要素間で各メッセージシンボルに関する信頼度情報を交換することで最適に近い復号特性を実現する方法論がTurbo（反復）復号 (iterative decoding) の基本的概念である．ここで一般にMAP復号器では各シンボルu_kに対し，符号のパリティ部による拘束条件から，外部情報（extrinsic information）と呼ばれるアナログ情報が生成される事実に着目する．

すなわち組織符号においては，あるシンボルu_kに関わる対数尤度比は以下の式によって表現されることが知られている[4].

$$L(\hat{u}_k) = L_c \cdot y_k + L(u_k) + L_e(\hat{u}_k). \tag{2}$$

ここで，

$L_c \cdot y_i$ ：受信信号値y_iから得られる通信路値（channel value），E_s/N_0をシンボル単位の信号対雑音電力比として

$$L_c = 4 \cdot E_s/N_0. \tag{3}$$

$L(u_k)$ ：$u_i = +1$と$u_i = -1$に関する既知の出現確率である事前確率 (*a priori* probability) $P(u_k)$の対数比 (*a priori* value).

$$\ln \frac{P(u_k = +1)}{P(u_k = -1)}. \tag{4}$$

$L_e(\hat{u}_k)$ ：符号のパリティ部に関する拘束条件により，u_kに関して得られる外部情報

一方の復号器で生成された外部情報 (Soft-Out) $L_e(\hat{u}_k)$を他方の復号器への入力 (Soft-In) させ，これを事前情報$L(u_k)$として新たにMAP復号を行なう操作を反復的に繰り返すことで，逐次的に特性の改善を図るboostrap手法が反復復号[2, 4]であり，ブロック図を図3に示す．図2に反復回数によるBER特性の改善が示されており，雑音レベルが高いほど多くの反復回数を要することが読みとれる．

なお，本復号法では$L^{(j)}(\hat{u}_k)$を他方の復号器とは独立な統計量として扱っているが，反復回数の増加に伴ってこの前提は必ずしも成立しないことに注意されたい．このため，インタリーバ長Nが小さい場合には確率の相関による影響で，ウォーターフォール領域でのBER特性の傾きは緩やかとなってしまう．

4 確率伝搬アルゴリズムと復号

前章で述べたように，反復復号法はTurbo符号に対して比較的ヒューリスティックに導入されたものであるが，その後，人工知能分野における確率推論のアルゴリズムと本質的に同一であることが知られるようになった．Turbo符号をメッセージ部とパリティ部からなる2部グラフで表現すると図4(a)のようになる．

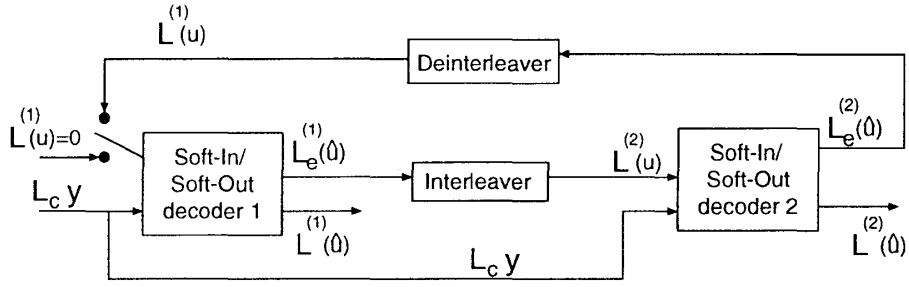

図 3: Turbo（反復）復号

Pearl の BP(Belief Propagation) アルゴリズム [5] は，Bayesian ネットワークにおいて親子ノード間で局所的な確率伝搬を行うことで，ループの存在しない Bayesian ネットワーク全体で正確な確率推論を行なうものである．この BP アルゴリズムを図 4(a) のネットワークに適用すると，反復復号同一のアルゴリズムが得られる [6, 7]．一方，Turbo 符号のグラフにはループが存在するが，BP アルゴリズムはこの種のネットワークでは正しい推定を行なわないため，人工知能工学分野ではあまり検討が行なわれていない．Turbo 符号の復号問題もあくまで実験的に良好な特性が観察されているにすぎず，かつ収束性も保証されないが，Turbo 符号化器におけるインタリーバが確率の相関が小さく抑えられるに足る大きさのループを生成する役割を担い，また基本的に復号の命題が事後確率ではなく，各メッセージノードにおける硬判定結果を得ればよい事実から，復号が成功しているものと考えられる．

1960 年代初頭に Gallager により発表された低密度パリティ検査 (LDPC) 符号 [3] が Turbo 符号の提案から間もなく再発見された．一般に線形符号は，すべての符号語$\boldsymbol{x}$に対して$\boldsymbol{x}H^T = \mathbf{o}$を満たす検査行列 Hにより定義されるが，LDPC 符号では極めて低密度のパリティ検査方程式，すなわち H中に “1” が疎に分布する．シミュレーションによる検証により，Gallager が示していた符号化復号法が Turbo 符号に近い特性を与えること，さらに重要なことに復号法が BP アルゴリズムの特別な場合として帰着されることが示された [8]．LDPC 符号のネットワークを図 4(b) に示す．この符号が 35 年に亙って忘れ去られた背景には，その後の代数的符号理論の発展や前述の縦列連接符号化の提案などがあるが，いずれにせよ，後の符号理論及び人工知能分野の大幅な発展を促した業績の本質部分を示していた事実は驚嘆に値する．

以上から，LDPC 符号で Shannon 限界に近い特性を得るには，BP アルゴリズムがより低い SNR で収束を開始するようなグラフ，すなわち符号を構成することが必須となる．Gallager が示した符号はノード間の接続数が均一であるグラフに相当するが，これを非正規 (irregular) グラフに拡張し，適切に設計することでより優れた特性を得ることが可能となる [9] ことが知られ，最適化が検討されている．従来符号理論では，BCH 符号や畳み込み符号などの距離構造に優れた符号の構成法が示され，その後 Berlekamp-Massey アルゴリズム，Viterbi アルゴリズムなどの効率的な復号法が与えられてきたが，グラフ上の符号に関しては明らかに方法論が異なっている．

確率伝搬アルゴリズムの収束性に関する理論は未だ未完成であるが，見通しの良い符号構成を与える意味において今後の研究にかかる期待は大きい．また，Turbo 符号や LDPC 符号に留まらず，様々なクラスの符号が同様の概念を用いて低複雑度で復号できることが示されており，さらに最尤復号規範に依っていた非同期検波，マルチユーザ検出，通信路等化といった広義の信号検出にも確率伝搬アルゴリズムは応用されており，通信理論における重要性は今後さらに増していくものと思われる．

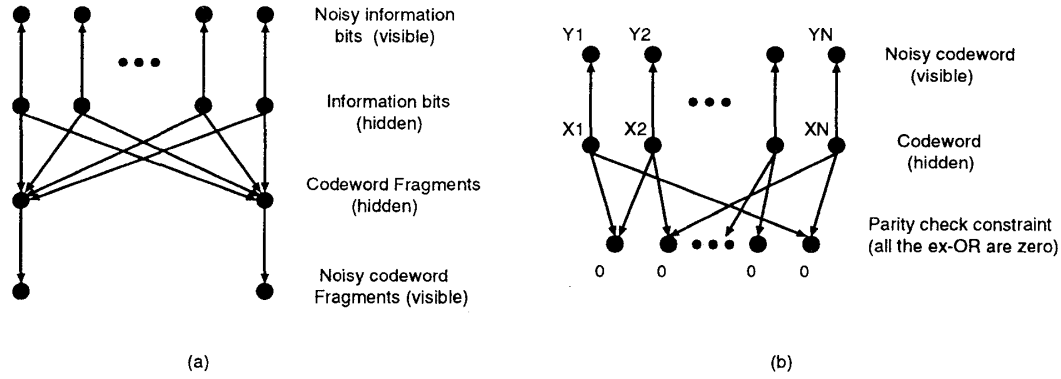

図 4: Bayesian ネットワーク (a) Turbo 符号, (b) 低密度パリティ検査符号

参考文献

[1] C.E. Shannon,"A mathematical theory of communication,"*Bell System Technical Journal*, vol.27, pp.379-423, July 1948 and pp.623-656, Oct. 1948.

[2] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding: Turbo codes,"in *Proc. of ICC93*, Geneva, Switzerland, pp.1064–1070, May 1993.

[3] R.G. Gallager,"Low-density parity-check codes,"*IRE Trans. Inform. Theory*, vol. IT-8, pp.21-28, Jan. 1962.

[4] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes, "*IEEE Trans. on Inform. Theory*, vol. 42, no.2, pp.429-445. March 1996.

[5] J. Pearl,"Probabilistic reasoning in intelligent systems: Networks of plausible inference,"San Mateo, CA: Morgan Kaufmann, 1988.

[6] R.J. McEliece, D.J.C. MacKay and J.-F. Cheng,"Turbo decoding as an instance of Pearl's "Belief Propagation"algorithm,"*IEEE J. Sel. Areas Commun.*, vol.16, no.2, pp.140-152, Feb. 1998.

[7] F. Kschischang and B. Frey,"Iterative decoding of compound codes by probability propagation in graphical models,"*IEEE J. Sel. Areas Commun.*, vol.16, no.2, pp.219-2230, Feb. 1998.

[8] D.J.C. MacKay and R.M. Neal,"Near Shannon limit performance of low density parity check codes, "*Electronics Lett.*, vol.32, pp.1645-1646, Aug. 1996.

[9] M. Luby, M. Mitzenmacher, A. Shokrollahi and D. Spielman, "Analysis of low density codes and improved designs using irregular graphs,"in *Proc. of the 30th annual ACM symposium on thoery of computing*, pp.249-258, 1998.